(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 047 215 A2

(12) # EUROPEAN PATENT APPLICATION

(43) Date of publication:
25.10.2000 Bulletin 2000/43

(51) Int. Cl.[7]: **H04J 11/00**

(21) Application number: 00303039.2

(22) Date of filing: 11.04.2000

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 19.04.1999 US 294165

(71) Applicant:
LUCENT TECHNOLOGIES INC.
Murray Hill, New Jersey 07974-0636 (US)

(72) Inventors:
- Giardina, Charles Robert
  Mahwah, New Jersey 07430 (US)
- Rudrapatna, Ashok N.
  Basking Ridge, New Jersey 07920 (US)

(74) Representative:
Buckley, Christopher Simon Thirsk et al
Lucent Technologies (UK) Ltd,
5 Mornington Road
Woodford Green, Essex IG8 0TU (GB)

## (54) A method of enhancing security for the transmission of information

(57) Quasi-Walsh function systems are developed which allow multiple access as well as spectral spreading for interception and jamming prevention. Mutual interference is minimal due to orthogonal spreading. High signal hiding capability occurs by utilizing a large number of distinct orthogonal codes. An encoding algorithm is presented which allows a simple way of "keeping track" of the different systems of Quasi-Walsh systems as well as determining appropriate values for given users at specified chip values.

FIG. 2

20

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = H^{*}D0 = Q0 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = H^{*}D1 = Q1 = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = H^{*}D2 = Q2 = \begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = H^{*}D3 = Q3 = \begin{pmatrix} -1 & -1 \\ -1 & -1 \end{pmatrix}$$

EP 1 047 215 A2

$$2^{2^n}.$$

Moreover, the same $D_k$ can occur numerous times in a single realization, thereby making a potentially large period for a resulting Pseudo Noise (PN) type sequence. The unique matrix $D_k$, post-multiplies H to give $Q_k = H D_k$. See FIG. 2 depicting an example of four possible systems of Quasi-Walsh functions $Q_k$ derived using the diagonal matrices $D_k$ of FIG. 1. Accordingly, the $i^{th}$ user is provisioned always the same $i^{th}$ row, however, it very likely comes from different Quasi-Walsh systems for each information bit transmitted. To an observer without knowledge of the formula for isometry generation, the resulting string of Quasi-Walsh functions seems random, thus hard to intercept.

[0007] Generalization to support larger than $2^n$ users is straightforward. We illustrate here the approach for supporting $2^{(n+1)}$ users; generalization to support users in excess of this follows the same logic. For each bit k, two D matrices are chosen, $D_k^1$ and $D_k^2$ such that all the Quasi-Walsh functions they produce are "almost orthogonal" with each other. The first $2^n$ users will be assigned Quasi-Walsh functions from $Q_k^1$ as described before and the next $2^n$ users from $Q_k^2$.

[0008] For any specific bit, the $i^{th}$ user is assigned the $i^{th}$ row involving Quasi-Walsh functions $Q_k$, whereas the $b^{th}$ user is assigned the $b^{th}$ row involving the same Quasi-Walsh functions $Q_k$. As a consequence, no mutual interference occurs since these codes are orthogonal. Thus, just like in a maximal length large shift register PN sequence, a long Quasi-Walsh type PN sequence can result across successive bits. This sequence of successive bits has all the signal hiding benefits as does a shift register sequence. In other words, the Quasi-Walsh functions $Q_k$ are changed across successive bits using an index, wherein the index may be determined using a PN sequence, an algorithm, a mathematical function, a known sequence, etc. Additionally, it has the added benefit of orthogonality resulting in ease of multiple access and acquisition. The length of the Quasi-Walsh PN sequence, before it repeats is a function of the length of the random number generator each of which determines the isometry of $D_k$. As an added degree of randomness the $i^{th}$ user at each bit may use a row other then the $i^{th}$. The actual row involving the Quasi-Walsh functions $Q_k$ can change (using another pseudo random number generator).

[0009] For a given $2^n x 2^n$ Walsh Hadamard matrix H,

$$2^{2^n}$$

distinct systems of Quasi-Walsh functions occur due to post multiplication by distinct diagonal isometrics $D_k$. The diagonal entries in these matrices will be interpreted in binary by replacing the minus ones on the diagonal by zeros. As a result, each distinct $D_k$ can be represented by an integer between 0 and

$$(2^{2^n} - 1).$$

Thus encoding, and correspondingly the decoding can be efficiently represented by the specific index k associated with each bit.

[0010] As a simplified illustration, consider the following example: In R2, two chips are used per single bit of information, and two users will be considered. In this case, n =1. Four distinct diagonal orthogonal matrices arise, as shown earlier in FIG. 1. When each of these matrices $D_k$ are applied to the Walsh-Hadamard matrix H by post multiplication, the systems of Quasi-Walsh functions $Q_k$ shown in FIG.2 are found.

[0011] To illustrate that for any realization consisting of all possible diagonal matrix isometrics an equal number of ones and minus ones occur, consider the following. Referring to the previous illustration, for each of the four bits of information transmitted, a diagonal matrix isometry is utilized. Suppose that an index specifics the isometrics $D_k$ in the following order: $D_0$, $D_1$, $D_2$, and $D_3$. Accordingly, the two chips used for modulating each bit transmitted are shown in FIG. 3. Note the equal number of 1 and —1 combinations both for User0 and User1.

[0012] The present invention is applicable to both Sylvester and non-Sylvester types. This permits operating in a non $2^n$ (n, integer) Real space The present Invention Is also applicable among non-orthogonal systems of Quasi-Walsh functions Q. Post multiplying Q by a permutation matrix P yields a generalized system of Quasi-Walsh function $Q^G$, i.e., $Q^G = H D P$. Note that here P has the same dimension (i.e., mxm) as H and D. Since, there are m! distinct Ps, the overall system of $Q^G$ increases by m! when compared to the system of Quasi-Walsh functions Q, improving the probability of finding cross system, low correlation generalized system of Quasi-Walsh functions, thereby yielding minimum mutual interference.

[0013] The process described above for assigning Quasi-Walsh functions works in the same manner for generalized systems of Quasi-Walsh functions $Q^G$, where $Q^G{}_j = H D_k P_x$. Where k = 1 to m (not necessarily equal to $2^n$) and x = 1 to m! Thus the specific generalized systems of Quasi-Walsh functions is defined by j, which is a function of the two-valued tuple {k, x}. Thus information hiding can be accomplished by the two-dimensional index or tuple {k, x}, enhancing information-hiding properties. In one realization, as described above each user would use the same specific row vector across all bits with each user using a different row with respect to each other. In this specific realization, spreading sequence for bit j would be selected from $Q^G{}_j$. Thus encoding, and correspondingly the

*FIG. 1*

<u>10</u>

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = D0$$

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = D1$$

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = D2$$

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = D3$$

*FIG. 2*

<u>20</u>

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = H^{*}D0 = Q0 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = H^{*}D1 = Q1 = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = H^{*}D2 = Q2 = \begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = H^{*}D3 = Q3 = \begin{pmatrix} -1 & -1 \\ -1 & -1 \end{pmatrix}$$

*FIG. 3*

<u>30</u>

| | Bit 1 | Bit 2 | Bit 3 | Bit 4 |
|---|---|---|---|---|
| FOR USER 0: | [1 1], | [1 −1], | [−1 1], | [−1 −1] |
| FOR USER 1: | [1 −1], | [1 1], | [−1 −1], | [−1 1] |

FPD 7/12

# PATENT COOPERATION TREATY

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To:
LADAS & PARRY
5670 WILSHIRE BOULEVARD
SUITE 2100
LOS ANGELES, CALIFORNIA 90036-5679

# PCT

## NOTIFICATION OF RECEIPT OF DEMAND BY COMPETENT INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

(PCT Rules 59.3(e) and 61.1(b), first sentence and Administrative Instructions, Section 601(a))

Date of mailing (*day/month/year*) 06 AUG 2002

**IMPORTANT NOTIFICATION**

Applicant's or agent's file reference 619372-0 09/730,697

| International application No. | International filing date (*day/month/year*) | Priority date (*day/month/year*) |
| --- | --- | --- |
| PCT/US01/46371 | 04 Dec 2001 | 05 Dec 2000 |

Applicant
GOSSETT, CARROLL, PHILIP

1. The applicant is hereby **notified** that this International Preliminary Examining Authority considers the following date as the date of receipt of the demand for international preliminary examination of the international application:

   0_ JUL 2002

2. That date of receipt is:

   - [x] the actual date of receipt of the demand by this Authority (Rule 61.1(b)).
   - [ ] the actual date of receipt of the demand on behalf of this Authority (Rule 59.3(e)).
   - [ ] the date on which this Authority has, in response to the invitation to correct defects in the demand (Form PCT/IPEA/404), received the required corrections.

3. [ ] **ATTENTION:** That date of receipt is **AFTER** the expiration of 19 months from the priority date. Consequently, the election(s) made in the demand does (do) not have the effect of postponing the entry into the national phase until 30 months from the priority date (or later in some Offices) (Article 39(1)). Therefore, the acts for entry into the national phase must be performed within 20 months from the priority date (or later in some Offices) (Article 22). For details, see the *PCT Applicant's Guide*, Volume II.

   [ ] *(If applicable)* This notification confirms the information given by telephone, facsimile transmission or in person on:

   ______________________________

4. Only where paragraph 3 applies, a copy of this notification has been sent to the International Bureau.

| Name and mailing address of the IPEA/ | Authorized officer |
| --- | --- |
| Assistant Commissioner for Patent, Box PCT<br>Washington, D.C. 20231 Attn:RO/US | MAMIE HOLMES Holmes, Mamie |
| Facsimile No. 703-305-3230 | Telephone No. 703-305-3664 |

Form PCT/IPEA/402 (July 1998)